thetac.tech

Darktrace Technical Assessment





tac

Note to Readers

Before the completion of this technical evaluation, MISI changed its name to Technology Advancement Center (TAC). The nonprofit conducting this report is now TAC, formerly known as MISI.

Introduction

As part of Technology Advancement Center's commitment to serving as an intermediary that helps connect U.S. Cyber Command (USCYBERCOM) and the U.S. government to the innovative products and solutions needed to advance the nation's cybersecurity capabilities, TAC offers third party technical evaluations to cybersecurity companies seeking testing and potential validation of their technology solutions. As an independent entity, TAC's technical evaluations and product assessments provide valuable feedback and industry credibility to emerging and well-established cybersecurity innovators. TAC understands there is no silver bullet for defense against any cybersecurity threat, and we recommend that any product or solution undergo continued testing and additional technical evaluations to evaluate its efficacy over time.

Executive Summary

In the fall of 2023, TAC completed a technical evaluation of the Darktrace Federal Cyber AI Mission Defense platform over a two-month period. The Darktrace Federal platform uses machine learning (ML) and artificial intelligence (AI) models and algorithms to detect and respond to anomalous behavior on a network.

TAC established evaluation criteria based on specific elements Darktrace Federal desired to be assessed against. With this in mind, we developed and executed a test plan against the platform using our proven testing methodology and the diverse skillset of our staff, to include offensive and defensive cyber operators and analysts and systems and network engineers. The TAC team deployed and implemented the Darktrace Federal platform into our lab environment and from the start we were impressed by the capabilities we tested and evaluated. The following assessment will provide additional context and data points.

Evaluation Criteria

The TAC team evaluated the Darktrace Federal Cyber AI Mission Defense platform on the following capabilities:

A. Ability to provide 100% visibility into network communications and asset identification regardless of protocol

B. Ability to provide 100% detection of anomalous behaviors, detect nation state-like attacks and APT threats all without rules, signatures or white/blacklisting

   I. Ease of human identification

   II. Ease of implementing unsupervised machine learning and artificial intelligence

C. Ability to provide a common single enforcement policy point across disparate IP transports (wireless, 5G, LAN)

D. Visibility before and after applying Darktrace Federal platform

   I. Verify obfuscation of IP address of all protected endpoints and devices

   II. Determine options to exploit OT environments using this solution

   III. Verify use of SAML and Multi factor authentication

   IV. Enforces a multi vector security framework.

E. Estimated level of expertise need to set-up and run including but not limited to:

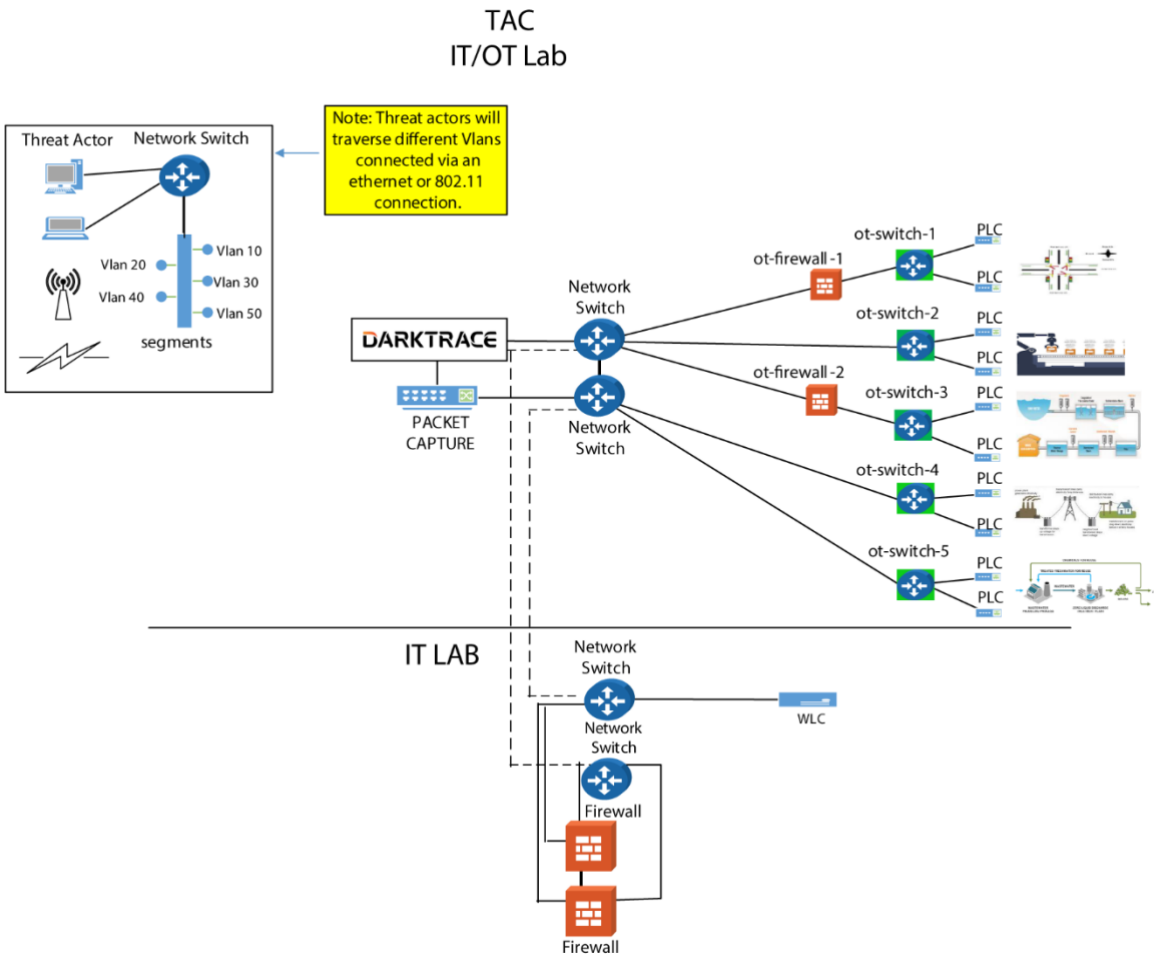
   I. Amount of local agents

II. Hardware devices

III. Time to complete operational training and deploy.

Network Configuration

The logical diagram below represents the lab network used for testing the Darktrace Federal platform.



Operating Systems Used

The following operating systems were used during the evaluation:

A. Kali Linux

B. Windows 11 Professional
C. Windows 10 Professional
D. MAC-OS
E. Windows 7 Ultimate
F. Window XP
G. Windows server 2012 Enterprise
H. Ubuntu 18.04
I. Ubuntu 20.04
J. Debain 9
K. K. Raspbian OS

Exploits deployed during the evaluation.

The TAC team deployed five exploits to test against the Darktrace Federal platform. A brief description of the exploits used are as follows:

A. **Exploit #1** Payload Distribution to Power Off a Programmable Logic Controller (PLC)

   We attempt to power off the electric grid in the lab OT using an ARP spoofing attack.

B. **Exploit #2** Wireless Sniffing & Wireless Key Cracking

   We attempt a deauthentication attack to exploit vulnerabilities in the wireless access points.

C. **Exploit #3** Lateral Movement and Data Exfiltration

   We attempt to extract files from a Windows Operating system exploiting the SMBv1 vulnerability.

D. **Exploit #4** Privilege Escalation Attack

   We attempt to use the RogueWinRM privilege escalation exploit to escalate from a service account to a local system account.

E. **Exploit #5** MODBUS Write Protocol Attack

We attempt to exploit native MODBUS protocol vulnerabilities to gain control of a Programmable Logic Controller (PLC) target that controls traffic lights in the lab OT network.

Testing Methodology and Results

Each attack assumes a breach has occurred, therefore focuses on the detection and response of the Darktrace Federal Cyber AI Mission Defense platform. We will highlight the various ways threats are discovered and presented to the analyst in the result.

Test #1 - **Exploit #1** Payload Distribution to Power Off a Programmable Logic Controller (PLC)

Attack Evolution: Attacker scans the network using Nmap and after successful identification of vulnerable devices executes script to exploit vulnerability remotely.

Result

Successful identification of breach. The Dynamic Threat Dashboard observes, chronicles and alerts on new activity and attack phases to include the following operations:

1. Suspicious network scan activity attempting to connect from the attacker device to the target device.
2. Failed connection attempts over various ports

Test #2 - **Exploit #2** Wireless Sniffing & Wireless Key Cracking

Attack Evolution: Attacker runs iwconfig then airmon-ng utility to enable monitoring mode on wireless interfaces. The attacker then analyzes the interface to locate a BSSID or ESSID of target wireless network. Attacker then attempts to run a de-auth attack on the identified ESSID by running aireplay-ng.

Result

Inconclusive. While Darktrace Federal was successful identifying new nodes connecting to the network at the time of the attack, it was unsuccessful in detecting the payload delivered by this attack. We determined a wireless interface would have been required on the appliance in order detect and analyze the rf signals from the wireless infrastructure to allow the platform to detect the de-auth and management frames to potentially identify this attack.

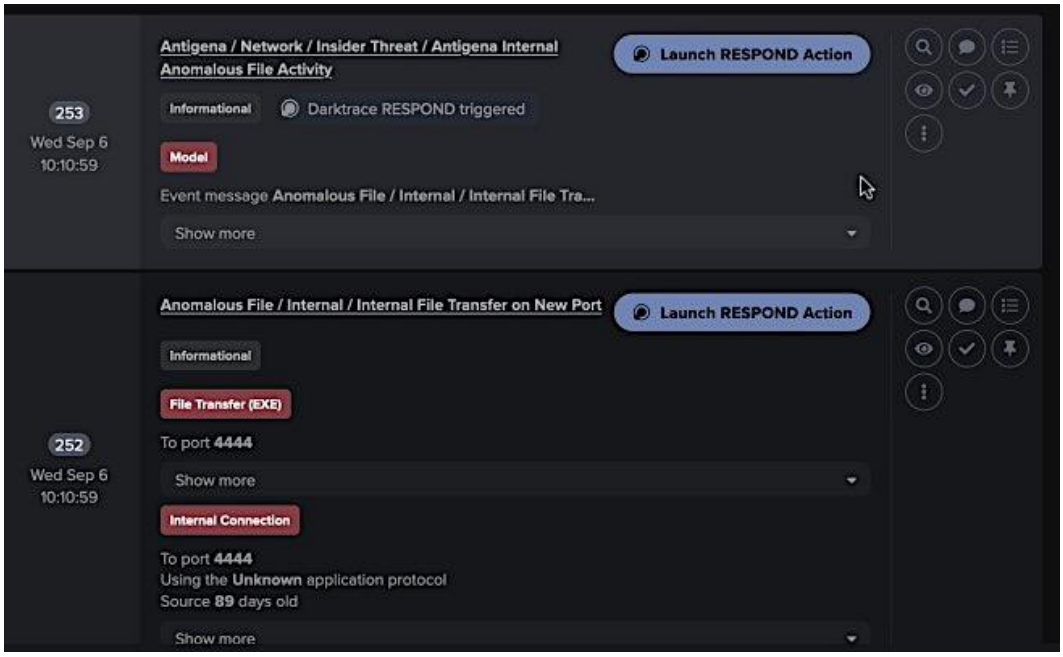
Test #3 - **Exploit #3** Data Exfiltration

Attack Evolution: Attacker runs port scan on subnet using NMAP. Attacker establishes persistence on vulnerable device via SSH session to find the device has been dual homed.

Attacker verifies connectivity to the target device by issuing a ping command. Attacker establishes connectivity to target and deploys and executes SMB exploit. The attacker searches for specific files on the target devices and begins exfiltration to the attacker's machine.

Result

Successful identification of breach. Using the Darktrace Federal Threat Visualizer, we opened an alert from the listed model breach section and gained additional insight into the breach as seen below:

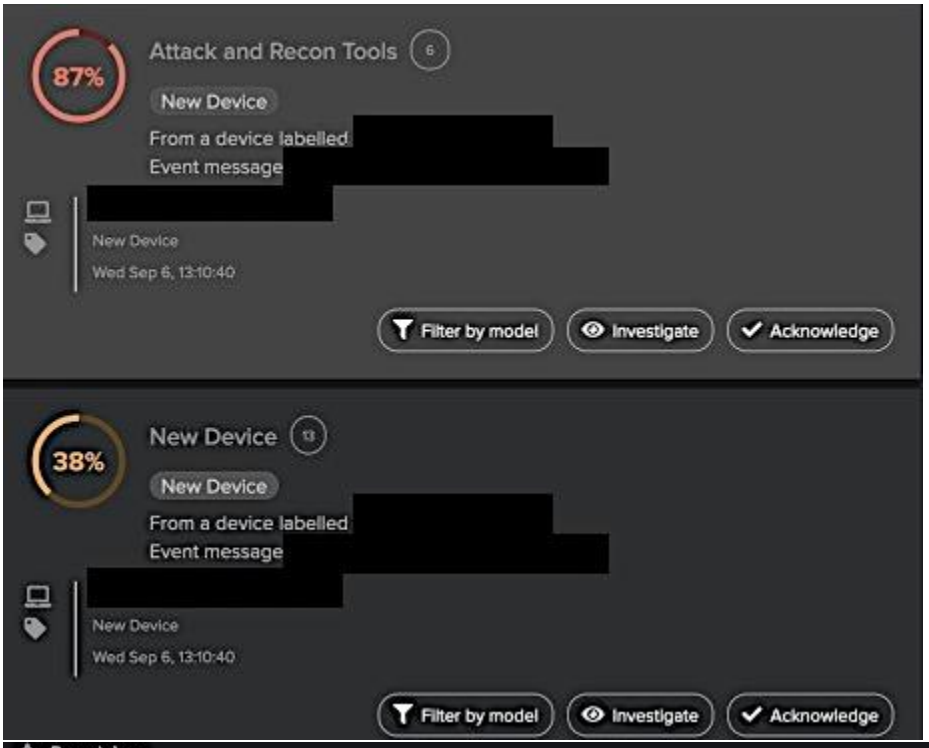


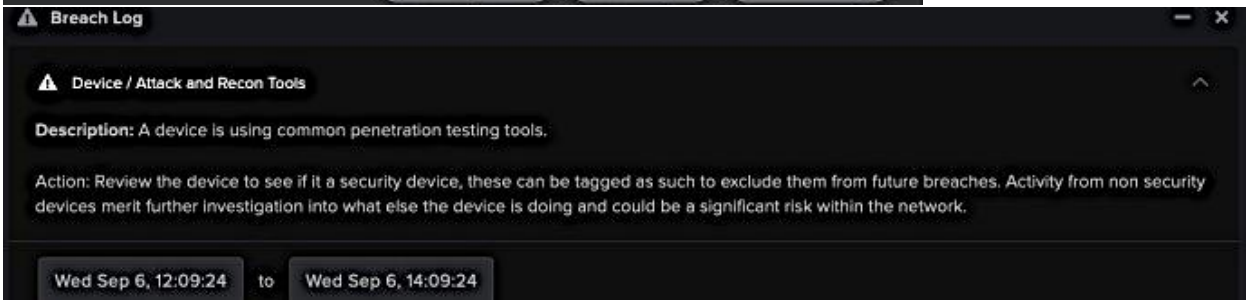
Test #4 - Exploit #4 Privilege Escalation Attack

Attack Evolution: Attacker establishes an RDP session to the target computer after acquiring credentials. Attacker opens PowerShell on target Windows computer. Attacker opens Netcat listener on Kali attack machine. Attacker launches the RogueWinRM executable on the target machine to initiate reverse shell to Netcat listener.

Result

Successful identification of breach. The Darktrace Federal Threat Visualizer identified attack and recon tools running on a new device on the network to include a threat score in addition to a recommended action to review the device to see if it is a known security device.



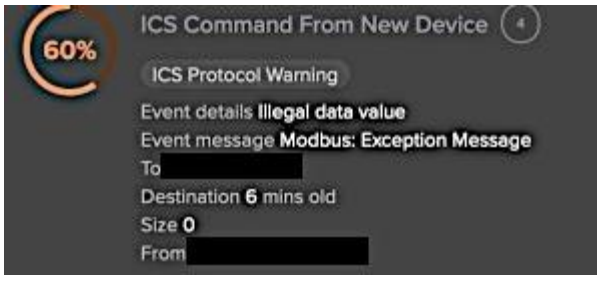


Test #5 - **Exploit #5** MODBUS Write Protocol Attack

Attack Evolution: Attacker conducts recon on possible targets using Nmap. Attacker sends Modbus commands against targets.

Result: **Successful identification of breach.**

The Darktrace Dynamic Threat Dashboard detects an ICS command issued from a new device to the target on the network. This was included with a recommendation to have the analyst identify other potential devices the breach device was attempting to communicate with.



Where Darktrace Federal Shines

Deployment

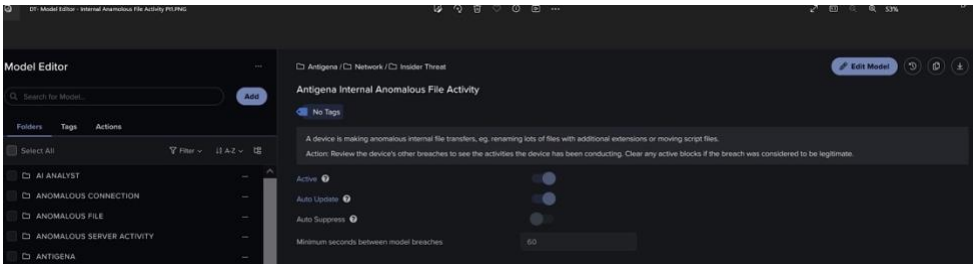
The installation of the on-prem physical appliance was simple and fast. A Darktrace Federal engineer unboxed and connected the device to the lab network. We supplied a management IP and then began to configure the appliance. We were completely online and ready to start discovery of the network in about one hour without the need to deploy any agents or sensors to endpoints or segments.

Network Discovery

An available analysis interface on the Darktrace Federal appliance was configured to use a **MIRROR** port on our distribution switch in the lab. We allocated two weeks for the appliance to learn about our network and its normal traffic patterns to include multi-cast and broadcast traffic. The platform was also successful in discovering each device type connected on our OT and IT networks including the nodes used during our testing. In the tests, the platform demonstrated the ability to provide 100% visibility into network communications and asset identification regardless of protocol, as established in the evaluation criteria.

Detecting and responding to threats in real time

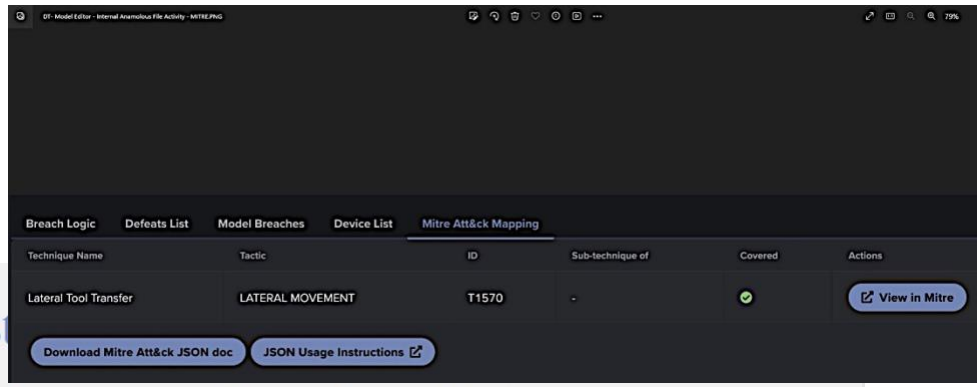
The Darktrace Federal Autonomous Response engine consistently detected and responded to attacks in real time, demonstrating its ability to provide 100% detection of anomalous behaviors as established in the evaluation criteria. During testing there were no observed false positives. During our limited testing we understand that traffic patterns will evolve and frequently change on the network, but we were encouraged by the possibility of not being inundated with less useful data.

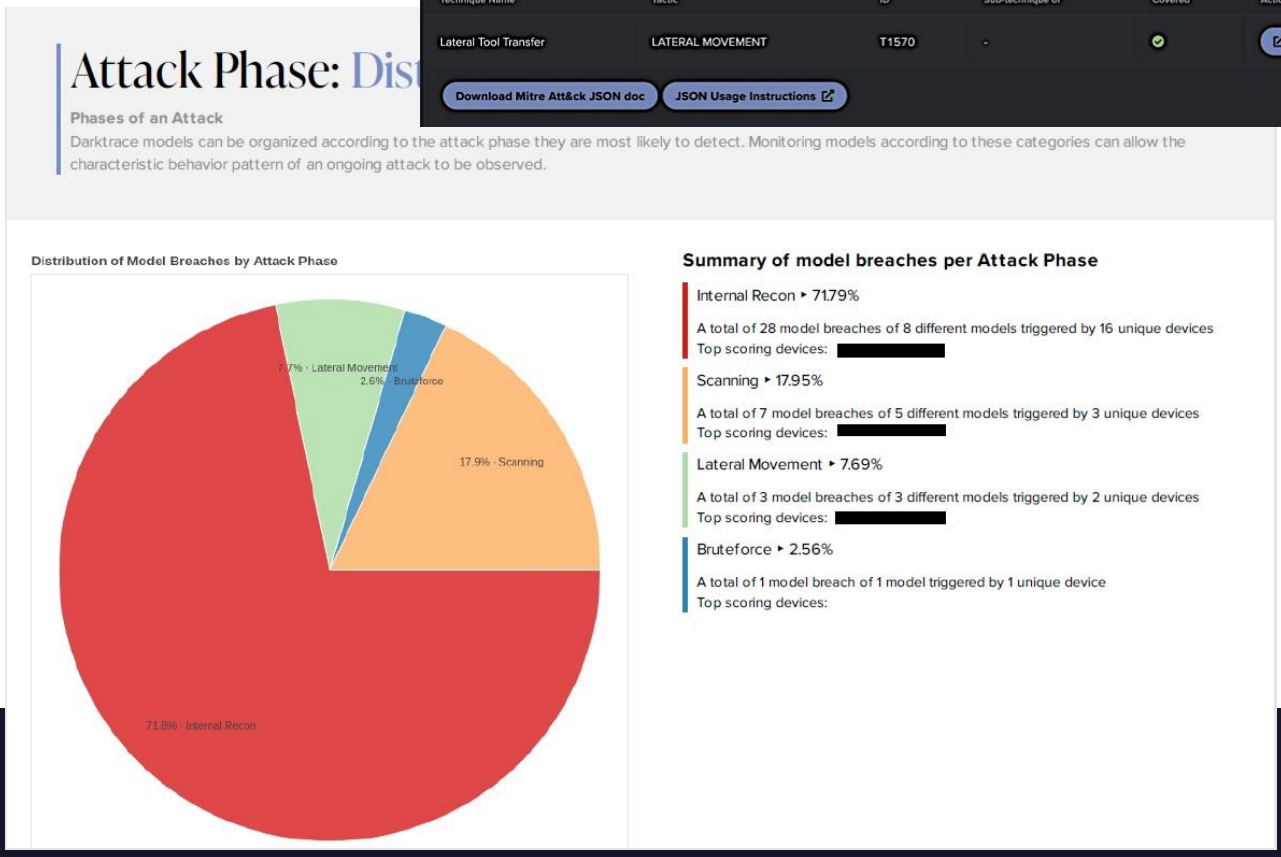


[See Darktrace Federal in action]

Also included with the engine is a model summary of threats detected during

TAC's testing. The results were accurately displayed. Within the model editor details of the breach and recommended





actions are displayed for the analyst to consider. The model editor takes it a step further, including a snap-in redirecting the analyst to the MITRE ATT&CK mapping knowledge-base for additional threat intelligence.

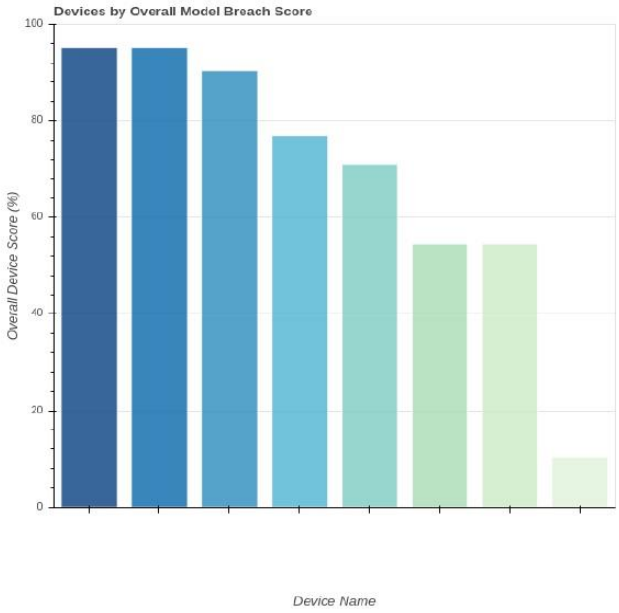
Reporting

Darktrace provides a detailed on-demand summary report chronicling the phases of attacks observed on the network.

Overall Score: Devices

Top Devices by Overall Score

Devices highlighted here have exhibited the greatest overall degree of unusual activity over the course of the reporting period. Device overall score gives an indication of which devices are at highest risk in the organisation.



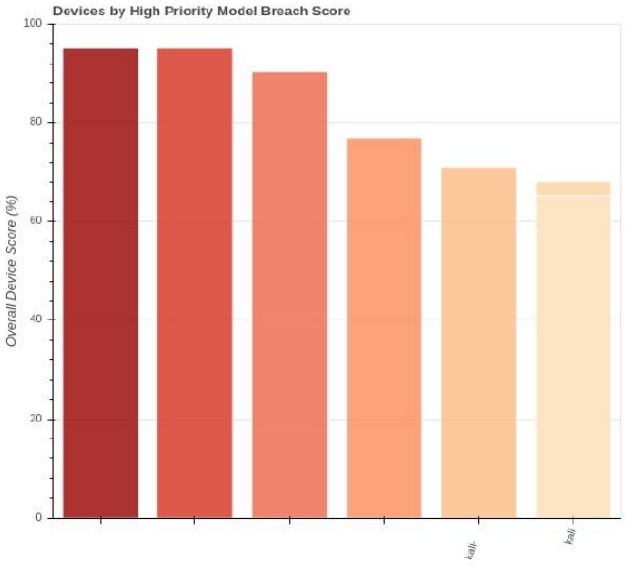
Devices Model Breach Summary

[redacted]	**Overall score: 95.10%**
Suspicious SMB Scanning Activity	87.26%
Anomalous Nmap Activity	87.26%
Large Number of Model Breaches	87.11%
[redacted]	**Overall score: 95.10%**
Suspicious Network Scan Activity	92.68%
Attack and Recon Tools	87.11%
New Device with Attack Tools	100.0%
[redacted]	**Overall score: 90.40%**
Network Scan	92.73%
[redacted]	**Overall score: 76.90%**
Attack and Recon Tools	87.23%
kali	**Overall score: 70.90%**
Attack and Recon Tools	87.11%
[redacted]	**Overall score: 54.60%**
DHCP Server	72.83%
[redacted]	**Overall score: 54.60%**
DHCP Server	72.81%
	Overall score: 10.40%
Multiple Devices Breaching Same Model	67.37%

High Priority Models: Devices

Top Devices Breaching High Priority Models

Devices highlighted here have breached models assessed to represent behaviors regarded as high priority for the organisation. This also includes models tagged by the customer using the 'Autoreporting' tag or model breaches with a score over 80%.



Devices Model Breach Summary

[redacted]	**Overall score: 95.10%**
Suspicious SMB Scanning Activity	87.26%
Large Number of Model Breaches	87.11%
Attack and Recon Tools	87.11%
[redacted]	**Overall score: 95.10%**
Attack and Recon Tools	87.11%
Suspicious Network Scan Activity	92.68%
New Device with Attack Tools	100.0%
[redacted]	**Overall score: 90.40%**
Network Scan	92.73%
[redacted]	**Overall score: 76.90%**
Attack and Recon Tools	87.23%
kali	**Overall score: 70.90%**
Attack and Recon Tools	87.11%
kali	**Overall score: 68.20%**
Attack and Recon Tools	87.09%
kali	**Overall score: 65.30%**
Attack and Recon Tools	87.11%

Where Darktrace Federal Can Improve

User Interface Navigation

The Darktrace Federal Threat Visualizer user interface (UI) takes some time to locate the data you may be looking for. Upon login you are presented with a global threat map displaying three-dimensional (3D) graphics that represent discovered subnets and additional graphics that provide a high-level analysis of the observed network activity to include detections and responses. From here you can start to drill down or search for additional insights.

While the data we would expect is certainly searchable and available, there are some overlapping menus and repetitive selections that return the same data but in a different view. This makes searches and configuring the platform unnecessarily complex.

An analyst wants fast access to the metrics that matter when investigating a possible breach. A small change like relocating the main menu from the analysis menu or consolidating it all into a single menu could go a long way.

Other AI threat detection tools evaluated in TAC's experience deliver simplified and intuitive interfaces, albeit at the expense of providing less threat intelligence compared to the level of threat intelligence included in the Darktrace Federal Platform. We would like to see more development towards an improved UI for future consideration.

Learning Curve

We recommend that organizations consider the various training options Darktrace Federal offers to get the most out of the platform. Darktrace Federal provided the TAC team with some foundational instruction and was able to provide answers to supplemental questions upon request.

The self-learning curve for our most experienced analyst was longer than expected. We were ultimately able to get comfortable enough to complete the evaluation without the need for formal instruction.

Conclusion

Because we were only able to test a limited amount of features of the Darktrace Federal Cyber Artificial Intelligence platform, we feel we only just scratched the surface of all its capabilities. It's worth noting that TAC observed additional technology integrations included in the platform, such as industry leading firewall manufacturers and cloud providers in addition to security integrations such as VirusTotal. These integrations can be useful for organizations where their security architectures allow for additional insight and response actions.



TAC feels the overall experience with this evaluation was largely positive. The time spent by our dedicated engineers delivered new learning opportunities and perspectives and also helped to reaffirm what we know and do so well as cybersecurity practitioners and cyber solution innovators.

The Darktrace Federal Cyber Artificial Intelligence platform successfully met the study's evaluation criteria, achieving 100% visibility into network communications, asset identification and 100% detection of anomalous behaviors.

Darktrace Federal's AI approach to network threat protection is mature and highly capable of detecting and mitigating emerging threats from their infancy stages to full evolution.

It is TAC's position that the Darktrace solution should be considered by organizations looking to complement or integrate with existing threat detection tools or deploy it during the early stages of a security and network infrastructure deployment to establish baselines as the environment evolves.



Technology Advancement Center (TAC), formerly MISI, is a cybersecurity nonprofit fueling the people and technology needed to solve critical cybersecurity challenges.

The TAC's three pillars of focus include: small business and academic engagement, STEM and workforce development, and proof of concept innovation.

Through collaboration with small businesses, academic researchers, and non-traditional members of the cybersecurity community, TAC serves as an intermediary and helps connect U.S. Cyber Command (USCYBERCOM) and the U.S. government to the innovative products and solutions needed to advance the nation's cybersecurity capabilities.

thetac.tech

tac